HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,315	07/28/2000	Kazuo Ezawa	AP32610-072817.0152	3474

21003 7590 01/24/2006

BAKER & BOTTS
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,315	EZAWA ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 14 October 2005.

2. Claims 1-58 are pending in the application.

3. Claims 1-58 have been rejected.

Response to Arguments

4. Applicant's arguments filed 14 October 2005 have been fully considered but they are not persuasive.

On page 15, the applicant argues that Ishiguro does not show, teach or suggest comparing "trusted times" on two cards and mutually replacing the "older" time on one of two cards with the "newer" time on the other card as is required by claim 37.

The examiner respectfully disagrees. The examiner asserts that there is no claim limitation of comparing "trusted times" on two cards. Ishiguro teaches updated an "older" time with the "newer" time with a time updating algorithm. However, the examiner asserts that there is no limitation of replacing the "older" time on one of two cards with the "newer" time on the *other card.*

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-44 and 46-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Ishiguro et al (USP 5,502,765).

As per claim 1, Ishiguro et al teaches a method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number (column 16 line 11 to column 17 line 16);

performing a verification using the first and second keys (column 6 line 13 to column 7 line 59);

if the second sequence number is newer than the first sequence number, setting the first sequence number to have a value of the second sequence number if the verification succeeds (column 16 line 11 to column 17 line 16); and conversely,

if the first sequence number is newer than the second sequence number, setting the second sequence number to have a value of the first sequence number if the verification succeeds (column 16 line 11 to column 17 line 16).

As per claims 25, Ishiguro et al teaches a portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receiving a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the portable device (column 16 line 11 to column 17 line 16),

comparing the first sequence number to the second sequence number (column 16 line 11 to column 17 line 16);

performing a verification using the first and second keys (column 6 line 13 to column 7 line 59);

if the second sequence number is newer than the first sequence number, setting the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first sequence number is newer than the second sequence number, setting the second sequence number to have a value of the first sequence number if the verification succeeds (column 16 line 11 to column 17 line 16).

As per claim 32, Ishiguro et al teaches a method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a

first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number (column 5, lines 52-53), wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the first portable device, the second sequence number being indicative of a second time provided on the second portable device (column 16 line 11 to column 17 line 16); and

if the first time is older than the second time, setting the first sequence number to have a value of the second sequence number and conversely (column 16 line 11 to column 17 line 16),

if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number (column 16 line 11 to column 17 line 16).

As per claims 37, Ishiguro et al teaches a portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device (column 16 line 11 to column 17 line 16),

compares the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the portable device, the second sequence number being indicative of a second time provided on the further portable device (column 16 line 11 to column 17 line 16), and executes one of the following actions:

if the first time is older than the second time, sets the first sequence number to have a value of the second sequence number and conversely (column 16 line 11 to column 17 line 16),

if the second time is older than the first time, sets the second sequence number to have a value of the first sequence number (column 16 line 11 to column 17 line 16).

As per claim 41, Ishiguro et al teaches a method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices (column 5, lines 52-53), the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the first portable device, the second sequence number being indicative of a second time provided on the second portable device (column 16 line 11 to column 17 line 16);

if the second time is newer than the first time, performing a verification using at least one of the first and second keys (column 16 line 11 to column 17 line 16); and

setting the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first time is newer than the second time, performing a verification using at least one of the first and second keys (column 16 line 11 to column 17 line 16); and

setting the second sequence number to have a value of the first sequence number if the verification succeeds (column 16 line 11 to column 17 line 16).

As per claim 54, Ishiguro et al teaches a portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device (column 16 line 11 to column 17 line 16),

compares the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the portable device, the second sequence number being indicative of a second time provided on the further portable device (column 16 line 11 to column 17 line 16),

if the second time is newer than the first time, performs a verification using the first and second keys (column 16 line 11 to column 17 line 16), and

sets the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first time is newer than the second time, performing a verification using at least one of the first and second keys (column 6 line 13 to column 7 line 59); and

setting the second sequence number to have a value of the first sequence number if the verification succeeds (column 16 line 11 to column 17 line 16).

As per claims 2, 31, and 58, Ishiguro et al teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 11 line 48 to column 12 line 7).

As per claim 3, Ishiguro et al teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 13, line 21-32).

As per claim 5, Ishiguro et al teaches after the setting step, performing a transaction between the first card and the second card (column 19, lines 29-50).

As per claim 6, Ishiguro et al teaches if the verification fails, suspending a transaction between the first card and the second card (column 18 line 41 to column 19 line 8).

As per claims 7, 26, 48, and 55, Ishiguro et al teaches if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device (column 18 line 41 to column 19 line 8).

As per claims 8, 27, and 58, Ishiguro et al teaches if the first sequence number and the second sequence number are equal, performing a transaction between the first card and the second card (column 19 line 29 to column 20 line 9).

As per claims 9 and 50, Ishiguro et al teaches wherein the setting step is performed by transmitting an authenticated system message ("ASM") command from the second card to the first card, and wherein at least one of the first and second cards sets the second sequence number (column 19 line 29 to column 20 line 9).

As per claims 10 and 28, Ishiguro et al teaches the first storage device stores a third sequence number thereon, wherein the second storage device stores a fourth sequence number

thereon (column 15 line 9 to column 16 line 30), and further comprising the steps of: if the first sequence number and the second sequence number are equal, determining whether the third sequence number corresponds to the fourth sequence number (column 15 line 9 to column 16 line 30); and if the third sequence number does not correspond to the fourth sequence number, transmitting an authenticated system message ("ASM") command from a particular card of the first and second cards having a newer number of the third and fourth sequence numbers to another card of the first and second cards (column 15 line 9 to column 16 line 30).

As per claim 11, Ishiguro et al teaches the ASM command is transmitted without setting the first sequence number to have the value of the second sequence number (column 15 line 9 to column 16 line 30).

As per claims 12 and 29, Ishiguro et al teaches if the third sequence number corresponds to the fourth sequence number, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claims 13 and 51, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number (column 16 line 11 to column 17 line 16).

As per claims 14 and 52, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the

second VTP key being stored in the second storage device (column 16 line 11 to column 17 line 16).

As per claims 15 and 53, Ishiguro et al teaches each of the first portable device and the second portable device includes a processing device (column 5, line 42-64).

As per claim 16, Ishiguro et al teaches receiving an authenticated system message which includes a command; and executing the command (column 6, lines 7-52).

As per claim 17, Ishiguro et al teaches providing an application to at least one card of the first and second cards, the application is provided for at least one of: renewing a security feature of the at least one card, and updating a security scheme of the at least one card on-chip management (column 21 line 64 to column 22 line 43).

As per claim 18, Ishiguro et al teaches providing a reference point for time to at least one of the first and second portable devices from a central command arrangement (column 5, line 42-64).

As per claim 19, Ishiguro et al teaches enabling a selective targeting of at least one device of the first and second portable devices (column 5, line 42-64); and applying re-customization procedures on the at least one device (column 5, line 42-64).

As per claim 20, Ishiguro et al teaches selecting a particular response by the at least one device when a predetermined criteria is met (column 21 line 64 to column 22 line 43).

As per claims 21 and 42, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing cryptograms which are related to the first global signing key and the second global key (column 16 line 11 to column 17 line 16).

As per claim 22, Ishiguro et al teaches generating the cryptograms by one of the first portable device and the second portable device (column 16 line 11 to column 17 line 16); and verifying the cryptograms using another one of the first portable device and the second portable device (column 16 line 11 to column 17 line 16).

As per claim 23, Ishiguro et al teaches the cryptograms are generated by a central authority (column 16 line 11 to column 17 line 16).

As per claims 24, Ishiguro et al teaches after the setting step, modifying stored parameters of at least one of the first and second cards to at least one of suspend, permit, and modify subsequent operations between the first and second cards or other cards (column 15 line 37 to column 16 line 44).

As per claims 30 and 57, Ishiguro et al teaches the portable device is a smart card, and wherein the further portable device is a further smart card (column 5, line 42-64).

As per claim 33, Ishiguro et al teaches if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number (column 15 line 9 to column 16 line 30).

As per claims 34 and 38, Ishiguro et al teaches after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number (column 15 line 9 to column 16 line 30).

As per claim 35, Ishiguro et al teaches after the executing step and, if the first time is not equal to the second time, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claims 36 and 49, Ishiguro et al teaches if the first time is equal to the second time, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claim 39, Ishiguro et al teaches wherein the portable device is a smart card, and the further portable device is a further smart card (column 5, line 42-64), and wherein, after the execution of the particular action and if the first time is not equal to the second time, the processing device performs a transaction between the smart card and the further smart card (column 15 line 9 to column 16 line 30).

As per claim 42, Ishiguro et al teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 16 line 11 to column 17 line 16).

As per claim 44, Ishiguro et al teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 15 line 9 to column 16 line 30).

As per claim 46, Ishiguro et al teaches after the setting step, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claim 47, Ishiguro et al teaches if the verification fails, suspending a transaction between the first card and the second card, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 4 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al in view of Carlisle et al (USP 5,649,118).

As per claims 4 and 45, Ishiguro et al teaches the method of encryption to secure the communication between two smart cards, as discussed above. Ishiguro et al fails to teach that the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys. Carlisle et al teach the use of public and private keys to secure the communication using smart cards (column 8, lines 31-45). Private key cryptography is well known in the art. Private key cryptography provides a very high level of security and is implemented in many applications.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Carlisle et of within the system of Ishiguro et al because private key encryption is well established in the art and can be implemented using smart cards as taught by Carlisle et al.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
January 20, 2006

Primary Examiner
AU2131
1/21/06